



## EMPFEHLUNG: IT IN UNTERNEHMEN

# Sichere Konfiguration von Microsoft Outlook

## für den Einsatz auf dem Betriebssystem Microsoft Windows

Büroanwendungen gehören in vielen Organisationen zu den am häufigsten genutzten Anwendungsprogrammen. Sie umfassen unter anderem Programme zur Textverarbeitung, Tabellenkalkulation und Erstellung von Präsentationen. Wegen ihrer großen Verbreitung und Angriffsfläche werden diese auch häufig als Angriffsweg genutzt, beispielsweise um mittels Makros in Office-Dokumenten Schadsoftware zu verbreiten und auf Zielsystemen auszuführen. Mit einer wohlüberlegten Konfiguration dieser Produkte kann das Risiko der Ausnutzung von Standardfunktionen oder Schwachstellen minimiert werden.

### Ziel

Hauptaugenmerk dieser Empfehlung liegt auf dem Einsatz von Microsoft Outlook in mittelgroßen bis großen Organisationen, in denen die Endsysteme mit Gruppenrichtlinien in einer Active Directory-Umgebung verwaltet werden. Alternativ können diese auch als lokale Sicherheitsrichtlinien angewendet werden. **Die Empfehlungen beziehen sich auf die Versionen 2016, 2019 und 2021 von Microsoft Outlook.** Bei Einsatz einer anderen Version lassen sich die Empfehlungen grundsätzlich für Entscheidungen zu einer Konfiguration unter Berücksichtigung möglicher Abweichungen ebenfalls heranziehen und anwenden.

Bei den vorliegenden Benutzerrichtlinien handelt es sich um Richtlinien von Microsoft Outlook, die sicherheitsrelevant sind. Weitere Einstellungen finden sich in den BSI-Veröffentlichungen:

- ✓ Sichere Konfiguration von Microsoft Access
- ✓ Sichere Konfiguration von Microsoft Excel
- ✓ Sichere Konfiguration von Microsoft Office
- ✓ Sichere Konfiguration von Microsoft PowerPoint
- ✓ Sichere Konfiguration von Microsoft Visio
- ✓ Sichere Konfiguration von Microsoft Word

### Sicherheitsprinzipien

Bei vielen Anwendungsprodukten ist die Konfiguration häufig ein Kompromiss aus Sicherheit und Funktionalität. Je mehr die Sicherheit in den Fokus gerückt wird, desto mehr wird die Benutzerfunktionalität damit eingeschränkt. Administratoren stehen immer vor der Herausforderung, hier die Ba-

lance zu finden und sollten die Konfiguration der Produkte und der benötigten Funktionalität von dem benötigten Schutzbedarf der verarbeiteten Informationen abhängig machen.

Für die Bereitstellung einer sicheren Standardanwendungsfunktionalität ist es demnach nicht einfach, organisationsübergreifende Empfehlungen zur Verfügung zu stellen, die in unterschiedlichen Anwendungsszenarien zum Einsatz kommen, sowie unterschiedliche Schutzbedürfnisse haben. Die Empfehlungen wurden daher anhand einer Reihe von Grundannahmen entwickelt, die im Folgenden kurz dargestellt werden:

- Für den Benutzer soll die Anzahl wichtiger Sicherheitsentscheidungen minimiert werden.
- Die benötigte Anwendungsfunktionalität soll nicht wesentlich beeinträchtigt werden.
- Nicht benötigte Funktionen sollen deaktiviert werden, um die Angriffsfläche zu verringern.
- Fokus auf Angriffsszenarien, die nach aktuellem Kenntnisstand auch ausgenutzt werden.
- Erhöhung des Datenschutzes, indem soweit wie möglich die Übertragungen von – für die Funktionalität nicht benötigte – Informationen an den Hersteller unterbunden wird.
- Erhöhung des Datenschutzes, indem externe Cloud-Dienste vermieden werden.

## Voraussetzungen

Die Sicherheit aller Microsoft Office-Produkte stützt sich auf die Sicherheit der Einsatzumgebung. Es wird daher vorausgesetzt, dass bereits

- entsprechende Richtlinien und bewährte Methoden zum Schutz der Organisationsinfrastruktur entwickelt wurden,
- aktuell branchenübliche Sicherheitstechniken eingesetzt werden sowie
- die im BSI-Grundschutz enthaltenen Empfehlungen und bewährten Methoden implementiert wurden.

## Gruppenrichtlinien

Im Folgenden werden die empfohlenen sicherheitsrelevanten Benutzerrichtlinien von Desktop- und Laptopcomputern aufgelistet. Diese können nur in Abhängigkeit von den Bedürfnissen innerhalb der Organisation umgesetzt werden. Wurde eine Active Directory-Umgebung innerhalb der gesamten Organisation bereitgestellt, auf denen die Office 2016-Version ausgeführt wird, können diese über eine Gruppenrichtlinie zentral verwaltet werden. Da die Beschreibungen der jeweiligen Richtlinien im Editor für Gruppenrichtlinien zu finden sind, wird auf eine Darstellung im Dokument verzichtet.

Richtlinien sind von Microsoft standardmäßig auf „Nicht konfiguriert“ voreingestellt. Je nach Richtlinie kann das entweder einer aktivierten oder deaktivierten Einstellung entsprechen. In einigen wenigen Fällen hat eine nicht konfigurierte Einstellung eine eigene Bedeutung. Darüber hinaus kann „Nicht konfiguriert“ bedeuten, dass dem Nutzer die Einstellung im Office-Programm selbst überlassen wird.

Da es prinzipiell möglich ist, dass sich durch Updates die Bedeutung von „Nicht konfiguriert“ ändert, sollten alle Richtlinien durch den Administrator immer auf „Aktiviert“ () oder „Deaktiviert“ () und nur im Ausnahmefall auf „Nicht konfiguriert“ () gesetzt werden. Rot markierte Einstellungen kennzeichnen, dass die BSI-Empfehlungen von der durch Microsoft festgelegten Bedeutung von „Nicht konfiguriert“ abweichen. Sollte bei Aktivierung der Richtlinie eine Auswahl oder Eingabe notwendig sein, befindet sich diese im Falle einer konkreten Empfehlung in der Fußnote.

<b>Besprechungsarbeitsbereich</b> <i>Meeting Workspace</i>		
1.	<b>Benutzereinträge in Serverliste deaktivieren</b> <i>Disable user entries to server list</i>	<input checked="" type="checkbox"/> <sup>1</sup>

<b>Outlook Connector für soziale Netzwerke</b> <i>Outlook Social Connector</i>		
2.	<b>Synchronisierung sozialer Netzwerkkontakte blockieren</b> <i>Block social network contact synchronization</i>	<input checked="" type="checkbox"/>
3.	<b>Synchronisierungsintervall für Aktivitätsfeeds angeben</b> <i>Specify activity feed synchronization interval</i>	<input checked="" type="checkbox"/> <sup>2</sup>
4.	<b>Synchronisierungsintervall für Kontakte der globalen Adressliste festlegen</b> <i>Set GAL contact synchronization interval</i>	<input checked="" type="checkbox"/> <sup>3</sup>
5.	<b>Fotos aus Active Directory nicht herunterladen</b> <i>Do not download photos from Active Directory</i>	<input checked="" type="checkbox"/>
6.	<b>Infoleisten sozialer Netzwerke nicht anzeigen</b> <i>Do not show social network info-bars</i>	<input checked="" type="checkbox"/>
7.	<b>Bestimmte Anbieter für soziale Netzwerke blockieren</b> <i>Block specific social network providers</i>	<input checked="" type="checkbox"/>
8.	<b>Synchronisierung der globalen Adressliste blockieren</b> <i>Block Global Address List synchronization</i>	<input type="checkbox"/>
9.	<b>Zu Liste der zu ladenden Anbieter für soziale Netzwerke angeben</b> <i>Specify list of social network providers to load</i>	<input checked="" type="checkbox"/>
10.	<b>Outlook Connector für soziale Netzwerke deaktivieren</b> <i>Turn off Outlook Social Connector</i>	<input checked="" type="checkbox"/>
11.	<b>Aktivitätssynchronisierung bei Bedarf nicht zulassen</b> <i>Do not allow on-demand activity synchronization</i>	<input checked="" type="checkbox"/>
12.	<b>Synchronisierung von Netzwerkaktivitäten blockieren</b> <i>Block network activity synchronization</i>	<input checked="" type="checkbox"/>
13.	<b>Office-Verbindungen mit sozialen Netzwerken deaktivieren</b> <i>Disable Office connections to social networks</i>	<input checked="" type="checkbox"/>

<b>Kontoeinstellungen\E-Mail</b> <i>Account Settings\E-mail</i>		
14.	<b>Speichern von Anmeldeinformationen mit Standardauthentifizierung verhindern</b> <i>Prevent saving credentials for Basic Authentication policy</i>	<input checked="" type="checkbox"/>

<b>Kontoeinstellungen\Exchange</b> <i>Account Settings\Exchange</i>		
15.	<b>RPC-Verschlüsselung aktivieren</b> <i>Enable RPC encryption</i>	<input checked="" type="checkbox"/>
16.	<b>Profil automatisch basierend auf der primären SMTP-Adresse von Active Directory konfigurieren</b> <i>Automatically configure profile based on Active Directory Primary SMTP address</i>	<input type="checkbox"/>

1 Veröffentlichungsstandard, andere nicht zulassen

2 60

3 5.760

17.	<b>Authentifizierung mit Exchange Server</b> <i>Authentication with Exchange Server</i>	<input checked="" type="checkbox"/> <sup>4</sup>
18.	<b>Benutzer können Ordnerberechtigungen nicht ändern</b> <i>Do not allow users to change permissions on folders</i>	<input checked="" type="checkbox"/>

<b>Kontoeinstellungen\Internetkalender</b> <i>Account Settings\Internet Calendars</i>		
19.	<b>Internetkalenderintegration nicht in Outlook einschließen</b> <i>Do not include Internet Calendar integration in Outlook</i>	<input checked="" type="checkbox"/>
20.	<b>Anlagen automatisch herunterladen</b> <i>Automatically download attachments</i>	<input type="checkbox"/>

<b>Kontoeinstellungen\RSS Feeds</b> <i>Account Settings\RSS Feeds</i>		
21.	<b>Anlagen automatisch herunterladen</b> <i>Automatically download enclosures</i>	<input type="checkbox"/>
22.	<b>RSS-Feature deaktivieren</b> <i>Turn off RSS feature</i>	<input type="checkbox"/>
23.	<b>Outlook-RSS-Feeds mit der gemeinsamen Feedliste synchronisieren</b> <i>Synchronize Outlook RSS Feeds with Common Feed List</i>	<input type="checkbox"/>
24.	<b>Vollständigen Text von Artikeln als HTML-Anlagen herunterladen</b> <i>Download full text of articles as HTML attachments</i>	<input type="checkbox"/>

<b>Elemente in Benutzeroberfläche deaktivieren\Benutzerdefiniert</b> <i>Disable Items in User Interface\Custom</i>		
25.	<b>Tastenkombinationen deaktivieren</b> <i>Disable shortcut keys</i>	<input type="checkbox"/>

<b>Verschiedenes</b> <i>Miscellaneous</i>		
26.	<b>Alle nicht verwalteten Add-ins blockieren</b> <i>Block all unmanaged add-ins</i>	<input checked="" type="checkbox"/>
27.	<b>Liste der verwalteten Add-Ins</b> <i>List of managed add-ins</i>	<input checked="" type="checkbox"/>
28.	<b>Kontaktgruppen nicht erweitern</b> <i>Do not expand Contact Groups</i>	<input type="checkbox"/>

<b>Verschiedenes\PST-Einstellungen</b> <i>Miscellaneous\PST Settings</i>		
29.	<b>PST-Daten beim Löschen nullen</b> <i>PST Null Data on Delete</i>	<input checked="" type="checkbox"/>

<b>Outlook-Optionen</b> <i>Outlook Options</i>		
---	--	--

4 Kerberos-Kennwortauthentifizierung

30.	<b>Internet- und Netzwerkpfade in Links konvertieren</b> <i>Internet and network paths into hyperlinks</i>	<input type="checkbox"/>
-----	---	--------------------------

**Outlook-Optionen\E-Mail-Format***Outlook Options\Mail Format*

31.	<b>Signaturen für E-Mail-Nachrichten nicht zulassen</b> <i>Do not allow signatures for e-mail messages</i>	<input checked="" type="checkbox"/>
-----	---	-------------------------------------

**Outlook-Optionen\E-Mail-Format\Internetformatierung***Outlook Options\Mail Format\Internet Formatting*

32.	<b>Outlook Rich-Text-Optionen</b> <i>Outlook Rich Text options</i>	<input checked="" type="checkbox"/>
33.	<b>Nur-Text-Optionen</b> <i>Plain text options</i>	<input type="checkbox"/>

**Outlook-Optionen\E-Mail\Internetformatierung\Nachrichtenformat***Outlook Options\Mail Format\Internet Formatting\Message Format*

34.	<b>Nachrichtenformat festlegen</b> <i>Set message format</i>	<input checked="" type="checkbox"/> <sup>5</sup>
-----	---	--

**Outlook-Optionen\E-Mail\Nachrichten verfassen***Outlook Options\Mail\Compose Messages*

35.	<b>Outlook-Schutzregeln</b> <i>Outlook Protection Rules</i>	<input checked="" type="checkbox"/>
-----	--	-------------------------------------

**Outlook-Optionen\Weitere***Outlook Options\Other*

36.	<b>Outlook als Standardprogramm für E-Mail, Kontakte und Kalender einrichten</b> <i>Make Outlook the default program for E-mail, Contacts, and Calendar</i>	<input checked="" type="checkbox"/>
-----	--	-------------------------------------

**Outlook-Optionen\Weitere\Erweitert***Outlook Options\Other\Advanced*

37.	<b>Ordner in anderen als Standardspeichern können nicht als Ordnerhomepages festgelegt werden</b> <i>Do not allow folders in non-default stores to be set as folder home pages</i>	<input checked="" type="checkbox"/>
38.	<b>Outlook-Objektmodellskripts können nicht für öffentliche Ordner ausgeführt werden</b> <i>Do not allow Outlook object model scripts to run for public folders</i>	<input checked="" type="checkbox"/>
39.	<b>Outlook-Objektmodellskripts können nicht für freigegebene Ordner ausgeführt werden</b> <i>Do not allow Outlook object model scripts to run for shared folders</i>	<input checked="" type="checkbox"/>
40.	<b>Unicode-Format beim Ziehen von E-Mail-Nachrichten in das Dateisystem verwenden</b> <i>Use Unicode format when dragging e-mail message to file system</i>	<input checked="" type="checkbox"/>

**Outlook-Optionen\Einstellungen\Junk-E-Mail***Outlook Options\Preferences\Junk E-mail*

5 Nur-Text

41.	<b>Junk-E-Mail-Schutzstufe</b> <i>Junk E-mail protection level</i>	<input checked="" type="checkbox"/> <sup>6</sup>
42.	<b>Benutzeroberfläche für Junk-E-Mail ausblenden</b> <i>Hide Junk Mail UI</i>	<input checked="" type="checkbox"/>
43.	<b>E-Mail von Kontakten vertrauen</b> <i>Trust e-mail from contacts</i>	<input checked="" type="checkbox"/>
44.	<b>E-Mail-Empfänger den Listen sicherer Absender der Benutzer hinzufügen</b> <i>Add e-mail recipients to users' Safe Senders Lists</i>	<input checked="" type="checkbox"/>
45.	<b>Warnungen zu verdächtigen Domännennamen in E-Mail-Adressen ausblenden</b> <i>Hide warnings about suspicious domain names in e-mail addresses</i>	<input checked="" type="checkbox"/>

<b>Outlook-Optionen\Einstellungen\E-Mail-Optionen</b> <i>Outlook Options\Preferences\E-mail Options</i>		
46.	<b>E-Mail als Nur-Text lesen</b> <i>Read e-mail as plain text</i>	<input checked="" type="checkbox"/>
47.	<b>Signierte E-Mail als Nur-Text lesen</b> <i>Read signed e-mail as plain text</i>	<input checked="" type="checkbox"/>

<b>Outlook-Optionen\Einstellungen\Kalenderoptionen\Office.com-Freigabedienst</b> <i>Outlook Options\Preferences\Calendar Options\Office.com Sharing Service</i>		
48.	<b>Veröffentlichen auf einem DAV-Server verhindern</b> <i>Prevent publishing to a DAV server</i>	<input checked="" type="checkbox"/>
49.	<b>Veröffentlichen auf Office.com verhindern</b> <i>Prevent publishing to Office.com</i>	<input checked="" type="checkbox"/>
50.	<b>Zugriff auf veröffentlichte Kalender</b> <i>Access to published calendars</i>	<input checked="" type="checkbox"/>
51.	<b>Hochlademethode einschränken</b> <i>Restrict upload method</i>	<input checked="" type="checkbox"/>
52.	<b>Kalenderdetails, die von Benutzern veröffentlicht werden können, einschränken</b> <i>Restrict level of calendar details users can publish</i>	<input checked="" type="checkbox"/> <sup>7</sup>

<b>Sicherheit</b> <i>Security</i>		
53.	<b>Add-In-Vertrauensebene konfigurieren</b> <i>Configure Add-In Trust Level</i>	<input checked="" type="checkbox"/> <sup>8</sup>
54.	<b>Antworten nicht automatisch signieren</b> <i>Do not automatically sign replies</i>	<input checked="" type="checkbox"/>
55.	<b>Einmalige ActiveX-Formulare zulassen</b> <i>Allow Active X One Off Forms</i>	<input checked="" type="checkbox"/> <sup>9</sup>
56.	<b>'Kennwort speichern' für Internet-E-Mail-Konten deaktivieren</b> <i>Disable 'Remember password' for Internet e-mail accounts</i>	<input checked="" type="checkbox"/>
57.	<b>Benutzer können Sicherheitseinstellungen für Anlagen nicht anpassen</b> <i>Prevent users from customizing attachment security settings</i>	<input checked="" type="checkbox"/>

6 Niedrig

7 Alle Optionen sind verfügbar

8 Alle geladenen und installierten COM-Add-Ins vertrauen

9 Nur Outlook-Steuerelemente laden

58.	<b>Geschützte Ansicht für Anlagen verwenden, die von internen Absendern empfangen wurden</b> <i>Use Protected View for attachments received from internal senders</i>	<input checked="" type="checkbox"/>
59.	<b>Aufforderung des Benutzers, Sicherheitseinstellungen auszuwählen, falls die Standardeinstellungen einen Fehler erzeugen</b> <i>Prompt user to choose security settings if default settings fail</i>	<input checked="" type="checkbox"/>
60.	<b>Exportieren von Kontakten deaktivieren</b> <i>Turn off contact export</i>	<input checked="" type="checkbox"/>

<b>Sicherheit\Einstellungen für den automatischen Download von Bildern</b> <i>Security\Automatic Picture Download Settings</i>		
61.	<b>Internet in sichere Zonen für den automatischen Download von Bildern einschließen</b> <i>Include Internet in Safe Zones for Automatic Picture Download</i>	<input checked="" type="checkbox"/>
62.	<b>Intranet in sichere Zonen für den automatischen Download von Bildern einschließen</b> <i>Include Intranet in Safe Zones for Automatic Picture Download</i>	<input checked="" type="checkbox"/>
63.	<b>Vertrauenswürdige Zonen blockieren</b> <i>Block Trusted Zones</i>	<input checked="" type="checkbox"/>
64.	<b>Herunterladen von Inhalt von sicheren Zonen nicht zulassen</b> <i>Do not permit download of content from safe zones</i>	<input checked="" type="checkbox"/>
65.	<b>Bilder und externen Inhalt in HTML-E-Mail anzeigen</b> <i>Display pictures and external content in HTML e-mail</i>	<input checked="" type="checkbox"/>
66.	<b>Automatisch Inhalt für E-Mail von Personen in den Listen 'Sichere Absender' und 'Sichere Empfänger' herunterladen</b> <i>Automatically download content for e-mail from people in Safe Senders and Safe Recipients Lists</i>	<input checked="" type="checkbox"/>

<b>Sicherheit\Kryptographie</b> <i>Security\Cryptography</i>		
67.	<b>S/MIME-Bestätigung anfordern, wenn mit S/MIME signiert</b> <i>Request an S/MIME receipt for all S/MIME signed messages</i>	<input checked="" type="checkbox"/>
68.	<b>Beschriftung aller mit S/MIME signierter Nachrichten sicherstellen</b> <i>Ensure all S/MIME signed messages have a label</i>	<input type="checkbox"/>
69.	<b>Fortezza-Zertifikatrichtlinien</b> <i>Fortezza certificate policies</i>	<input checked="" type="checkbox"/>
70.	<b>S/MIME-Interoperabilität mit externen Clients</b> <i>S/MIME interoperability with external clients:</i>	<input checked="" type="checkbox"/> <sup>10</sup>
71.	<b>Alle E-Mail-Nachrichten signieren</b> <i>Sign all e-mail messages</i>	<input checked="" type="checkbox"/>
72.	<b>Antworten auf bzw. Weiterleitungen von signierten/verschlüsselten Nachrichten sind signiert/verschlüsselt</b> <i>Replies or forwards to signed/encrypted messages are signed/encrypted</i>	<input checked="" type="checkbox"/>
73.	<b>URL für S/MIME-Zertifikate</b> <i>URL for S/MIME certificates</i>	<input checked="" type="checkbox"/>
74.	<b>Immer TNEF-Formatierung in S/MIME-Nachrichten verwenden</b> <i>Always use TNEF formatting in S/MIME messages</i>	<input checked="" type="checkbox"/>
75.	<b>Option 'Weiter' in Dialogfeldern mit Verschlüsselungswarnungen nicht bereitstellen</b> <i>Do not provide Continue option on Encryption warning dialog boxes</i>	<input checked="" type="checkbox"/>

10 Soweit möglich verarbeiten

76.	<b>Alle signierten Nachrichten als Klartext senden</b> <i>Send all signed messages as clear signed messages</i>	<input checked="" type="checkbox"/>
77.	<b>Nachrichtenformate</b> <i>Message Formats</i>	<input checked="" type="checkbox"/>
78.	<b>Schaltfläche 'In GAL veröffentlichen' nicht anzeigen</b> <i>Do not display 'Publish to GAL' button</i>	<input checked="" type="checkbox"/>
79.	<b>Signaturwarnung</b> <i>Signature Warning</i>	<input checked="" type="checkbox"/> <sup>11</sup>
80.	<b>SuiteB-Algorithmen sind für S/MIME-Vorgänge erforderlich</b> <i>Require SuiteB algorithms for S/MIME operations</i>	<input checked="" type="checkbox"/>
81.	<b>E-Mail-Adresse nicht mit der Adresse von verwendeten Zertifikaten vergleichen</b> <i>Do not check e-mail address against address of certificates being used</i>	<input checked="" type="checkbox"/>
82.	<b>Kryptografiesymbole aktivieren</b> <i>Enable Cryptography Icons</i>	<input checked="" type="checkbox"/>
83.	<b>Im FIPS-kompatiblen Modus ausführen</b> <i>Run in FIPS compliant mode</i>	<input checked="" type="checkbox"/>
84.	<b>Mindestverschlüsselungseinstellungen</b> <i>Minimum encryption settings</i>	<input checked="" type="checkbox"/> <sup>12</sup>
85.	<b>Alle E-Mail-Nachrichten verschlüsseln</b> <i>Encrypt all e-mail messages</i>	<input type="checkbox"/>
86.	<b>Erforderliche Zertifizierungsstelle</b> <i>Required Certificate Authority</i>	<input checked="" type="checkbox"/>
87.	<b>S/MIME-Bestätigungsanforderungsverhalten</b> <i>S/MIME receipt requests behavior</i>	<input checked="" type="checkbox"/> <sup>13</sup>
88.	<b>Auf den privaten Schlüssel des Benutzers überprüfen, wenn dieser eine verschlüsselte E-Mail sendet, die den Benutzer als Empfänger enthält</b> <i>Check for the user's private key when the user sends an encrypted email that includes the user as a recipient</i>	<input checked="" type="checkbox"/>

<b>Sicherheit\Kryptographie\Dialogfeld 'Signaturstatus'</b> <i>Security\Cryptography\Signature Status dialog box</i>		
89.	<b>Abrufen von Zertifikatsperrlisten</b> <i>Retrieving CRLs (Certificate Revocation Lists)</i>	<input checked="" type="checkbox"/> <sup>14</sup>
90.	<b>Anlage sicherer temporärer Ordner</b> <i>Attachment Secure Temporary Folder</i>	<input checked="" type="checkbox"/>
91.	<b>Fehlende Stammzertifikate</b> <i>Missing root certificates</i>	<input checked="" type="checkbox"/> <sup>15</sup>
92.	<b>Fehlende Zertifikatsperrlisten</b> <i>Missing CRLs</i>	<input checked="" type="checkbox"/> <sup>16</sup>
93.	<b>Fehler der Ebene 2 als Fehler, nicht als Warnungen, höher stufen</b> <i>Promote Level 2 errors as errors, not warnings</i>	<input checked="" type="checkbox"/>

### Sicherheit\Sicherheitsformulareinstellungen

11 Immer wegen ungültigen Signaturen warnen

12 256

13 Nachricht öffnen, wenn Bestätigung nicht gesendet werden kann

14 Im Onlinemodus immer die Zertifikatsperrliste abrufen

15 Fehler

16 Fehler



Security\Security Form Settings		
94.	<b>Outlook-Sicherheitsmodus</b> <i>Outlook Security Mode</i>	<input checked="" type="checkbox"/> <sup>17</sup>

Sicherheit\Sicherheitsformulareinstellungen\Anlagensicherheit Security\Security Form Settings\Attachment Security		
95.	<b>Als Ebene 1 blockierte Dateierweiterungen entfernen</b> <i>Remove file extensions blocked as Level 1</i>	<input checked="" type="checkbox"/>
96.	<b>Als Ebene 1 zu blockierende Dateierweiterungen hinzufügen</b> <i>Add file extensions to block as Level 1</i>	<input checked="" type="checkbox"/>
97.	<b>Als Ebene 2 blockierte Dateierweiterungen entfernen</b> <i>Remove file extensions blocked as Level 2</i>	<input checked="" type="checkbox"/>
98.	<b>Als Ebene 2 zu blockierende Dateierweiterungen hinzufügen</b> <i>Add file extensions to block as Level 2</i>	<input checked="" type="checkbox"/>
99.	<b>Anlagen der Ebene 1 anzeigen</b> <i>Display Level 1 attachments</i>	<input checked="" type="checkbox"/>
100.	<b>Benutzer können Anlagen auf Ebene 2 tiefer stufen</b> <i>Allow users to demote attachments to Level 2</i>	<input checked="" type="checkbox"/>
101.	<b>Keine Eingabeaufforderung zu Anlagen der Ebene 1 beim Schließen eines Elements</b> <i>Do not prompt about Level 1 attachments when closing an item</i>	<input checked="" type="checkbox"/>
102.	<b>Keine Eingabeaufforderung zu Anlagen der Ebene 1 beim Senden eines Elements</b> <i>Do not prompt about Level 1 attachments when sending an item</i>	<input checked="" type="checkbox"/>
103.	<b>OLE-Paketobjekte anzeigen</b> <i>Display OLE package objects</i>	<input checked="" type="checkbox"/>

Sicherheit\Sicherheitsformulareinstellungen\Benutzerdefinierte Formularensicherheit Security\Security Form Settings\Custom Form Security		
104.	<b>Ausführungseingabeaufforderung für Outlook-Objektmodell 'Benutzerdefinierte Aktionen' festlegen</b> <i>Set Outlook object model custom actions execution prompt</i>	<input checked="" type="checkbox"/> <sup>18</sup>
105.	<b>Skripts in einmaligen Outlook-Formularen zulassen</b> <i>Allow scripts in one-off Outlook forms</i>	<input checked="" type="checkbox"/>

Sicherheit\Sicherheitsformulareinstellungen\Programmatische Sicherheit Security\Security Form Settings\Programmatic Security		
106.	<b>Eingabeaufforderung für Outlook-Objektmodell beim Antworten auf Besprechungs- und Aufgabenanfragen</b> <i>Configure Outlook object model prompt when responding to meeting and task requests</i>	<input checked="" type="checkbox"/> <sup>19</sup>
107.	<b>Eingabeaufforderung für Outlook-Objektmodell beim Zugriff auf ein Adressbuch konfigurieren</b> <i>Configure Outlook object model prompt when accessing an address book</i>	<input checked="" type="checkbox"/> <sup>20</sup>

17 Outlook-Sicherheitsgruppenrichtlinie verwenden

18 Automatisch ablehnen

19 Automatisch ablehnen

20 Automatisch ablehnen

108.	<b>Eingabeaufforderung für Outlook-Objektmodell beim Lesen von Adressinformationen konfigurieren</b> <i>Configure Outlook object model prompt when reading address information</i>	<input checked="" type="checkbox"/> <sup>21</sup>
109.	<b>Eingabeaufforderung für Outlook-Objektmodell beim Zugriff auf die Formel-Eigenschaft eines UserProperty-Objekts konfigurieren</b> <i>Configure Outlook object model prompt When accessing the Formula property of a UserProperty object</i>	<input checked="" type="checkbox"/> <sup>22</sup>
110.	<b>Eingabeaufforderung für Outlook-Objektmodell beim Ausführen von 'Speichern unter' konfigurieren</b> <i>Configure Outlook object model prompt when executing Save As</i>	<input checked="" type="checkbox"/> <sup>23</sup>
111.	<b>Eingabeaufforderung für Outlook-Objektmodell beim Senden von E-Mail konfigurieren</b> <i>Configure Outlook object model prompt when sending mail</i>	<input checked="" type="checkbox"/> <sup>24</sup>
112.	<b>Eingabeaufforderung für die Namensauflösung für Simple MAPI konfigurieren</b> <i>Configure Simple MAPI name resolution prompt</i>	<input checked="" type="checkbox"/> <sup>25</sup>
113.	<b>Eingabeaufforderung zum Öffnen von Nachrichten für Simple MAPI konfigurieren</b> <i>Configure Simple MAPI message opening prompt</i>	<input checked="" type="checkbox"/> <sup>26</sup>
114.	<b>Simple MAPI-Sendeaufforderung konfigurieren</b> <i>Configure Simple MAPI sending prompt</i>	<input checked="" type="checkbox"/> <sup>27</sup>

**Sicherheit\Sicherheitsformulareinstellungen\Programmatische Sicherheit\Vertrauenswürdige Add-Ins**  
*Security\Security Form Settings\Programmatic Security\Trusted Add-ins*

115.	<b>Vertrauenswürdige Add-Ins konfigurieren</b> <i>Configure trusted add-ins</i>	<input type="checkbox"/>
------	--	--------------------------

**Sicherheit\Trust Center**  
*Security\Trust Center*

116.	<b>Links in verdächtigen Phishing-E-Mail-Nachrichten zulassen</b> <i>Allow hyperlinks in suspected phishing e-mail messages</i>	<input type="checkbox"/>
117.	<b>Sicherheitseinstellung für Makros</b> <i>Security setting for macros</i>	<input checked="" type="checkbox"/> <sup>28</sup>
118.	<b>Makrosicherheitseinstellungen auf Makros, Add-Ins und zusätzliche Aktionen anwenden</b> <i>Apply macro security settings to macros, add-ins and additional actions</i>	<input checked="" type="checkbox"/>
119.	<b>Senden blockieren, wenn Web-Add-Ins nicht geladen werden können</b> <i>Block send when web add-ins can't load</i>	<input type="checkbox"/>
120.	<b>Aktivierungsaufhebungsschwelle für Web-Weiterungen angeben</b> <i>Specify activation disabling threshold for web extensions</i>	<input checked="" type="checkbox"/> <sup>29</sup>
121.	<b>Wiederholungsgrenzwert für Aktivierungsmanager für Web-Weiterungen angeben</b> <i>Specify activation manager retry limit for web extensions</i>	<input checked="" type="checkbox"/> <sup>30</sup>
122.	<b>Warnintervall für Web-Weiterungen angeben</b> <i>Specify alert interval for web extensions</i>	<input checked="" type="checkbox"/> <sup>31</sup>

21 Automatisch ablehnen

22 Automatisch ablehnen

23 Automatisch ablehnen

24 Automatisch ablehnen

25 Eingabeaufforderung für Benutzer

26 Eingabeaufforderung für Benutzer

27 Eingabeaufforderung für Benutzer

28 Mit Vorzeichen warnen, ohne Vorzeichen deaktivieren

29 1000

30 3

31 5

123.	<b>Outlook-Speicherwarnschwelle für Weberweiterungen angeben</b> <i>Specify Outlook memory alert threshold for web extensions</i>	<input checked="" type="checkbox"/> <sup>32</sup>
124.	<b>Anzahl der versuchten Neustarts für eine ausgeführte Weberweiterung angeben</b> <i>Specify the number of restarts attempted for a running web extension</i>	<input checked="" type="checkbox"/> <sup>33</sup>

## Restrisiken

Die Konfiguration der Gruppenrichtlinien hilft nur dabei, die Angriffsfläche auf Anwendungen von Microsoft Outlook zu verringern bzw. die Sicherheit zu erhöhen. So existieren beispielsweise Verhaltensweisen, die nicht mittels Gruppenrichtlinien konfigurierbar sind. So können beispielsweise durch die Telemetrie auch sensible Daten an Microsoft übertragen werden.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an [info@cyber-allianz.de](mailto:info@cyber-allianz.de) gesendet werden.

<sup>32</sup> 1500

<sup>33</sup> 3